

## INFORMATION DISCLOSURE CITATION

Atty. Docket No.	04329.2163-01	Appln. No.	To be Assigned
Applicant	Fumihiko SANO et al.		
Filing Date	Concurrently Herewith	Parent Group:	2131 3621

## U.S. PATENT DOCUMENTS

Examiner Initial*	Document Number	Issue Date	Name	Class	Sub Class	Filing Date If Appropriate
SP	3,962,538	06/08/76	Ehrsam et al.	/	/	
SP	5,231,662	07/1993	van Rumpt et al.	/	/	
SP	4,157,454	06/1979	Becker	/	/	
SP	5,778,074	07/1998	Garcken et al.	/	/	
SP	6,570,989	05/2003	Ohmori et al.	/	/	
SP	5,623,549	04/1997	Ritter	/	/	
SP	5,768,390	06/1998	Coppersmith et al.	/	/	
SP	5,606,616	02/1997	Sprunk et al.	/	/	
SP	5,454,039	09/1995	Coppersmith et al.	/	/	
SP	5,623,548	04/1997	Akiyama et al.	/	/	

## FOREIGN PATENT DOCUMENTS

Document Number	Publication Date	Country	Class	Sub Class	Translation Yes or No
SP 10-116029	05/06/1998	Japan			Abstract
SP 51-108701	9/27/1976	Japan			Partial Translation

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

SP	E. Biham et al., "How to strengthen DES using existing hardware," Advances in Cryptology - ASIACRYPT'94, 4 <sup>th</sup> International Conference on the theory and applications of cryptology.
SP	Proceedings, Advances in Cryptology - ASIACRYPT-94, 4 <sup>th</sup> International Conference on the theory and applications of cryptology, Wollongong, pp. 398-412, XP000527605, 1995, Berlin, Germany, Springer-Verlag.
SP	M. H. Dawson et al., "An expanded set of design criteria for substitution boxes and their use in strengthening DES-like cryptosystems," IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (Cat. No. 91CH2954-6), Victoria, BC, Canada, 9-10 May 1991, pp. 191-195, vol. 1 XP000280289, 1999.
SP	American National Standard, "X.9.52 - 1998, Triple Data Encryption Algorithm Modes Of Operation," American Bankers Association, Pages 1-89, 1998.
SP	Fumihiko Sano and Kouichi Sakurai, "DES Compatible 128-bits Key Block Cipher DES-SS."

## INFORMATION DISCLOSURE CITATION

Atty. Docket No.	04329.2163-01	Appln. No.	To be Assigned
Applicant	Fumihiko SANO et al.		
Filing Date	Concurrently Herewith	Parent Group:	2131

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)	
<i>SR</i>	"Proceedings of the 19 <sup>th</sup> Symposium on Information Theory and Its Application," December 3-6, 1996, Vol. 2, IEEE Information Theory Society, Tokyo Chapter.
<i>SR</i>	E. Biham and A. Shamir, "Differential Cryptanalysis of DES-Like Cryptosystems," Journal of Cryptology, Vol. 4, Number 1, 1991.
<i>SR</i>	Mitsuru Matsui, "Linear Cryptanalysis of DES Cipher (I)," Encryption and Information Security Symposium, 1993.
<i>SR</i>	Bruce Schneier, Applied Cryptography, Second Edition, 1996, John Wiley & Sons, Inc.

Examiner	<i>S. Cangelosi</i>	Date Considered	<i>1/06</i>
*Examiner:	Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.		
Form PTO 1449		Patent and Trademark Office - U.S. Department of Commerce	